CLAIMS:

1. A method of secret key agreement between a first (16) and a second (18) correspondent, the method comprising the acts of:

(a) said first correspondent receiving a response A, from a source P (20);

(b) said second correspondent receiving a response B from said source P (20);

(c) said first correspondent generating (d-1) parity symbols as an output of a codeword W whose input includes said response A and a secret key K selected by said first correspondent (16);

(d) said first correspondent (16) transmitting said (d-1) parity symbols over a public communication channel (22) to said second correspondent (18); and

(e) said second correspondent (18) generating a word W' whose input includes said (d-1) parity symbols and said response B to determine said secret key K.

2. The method of Claim 1, wherein said responses A and B are received by said respective first (16) and second (18) correspondents responsive to a challenge C generated from said respective first (16) and second (18) correspondents.

3. The method of Claim 1, wherein said response A is comprised of a sequence of symbols of the form $A=(a_1,\ldots\ldots a_n)$.

4. The method of Claim 1, wherein said response B is comprised of a sequence of symbols of the form B=(b1,.....,bn).

5. The method of Claim 1, wherein said secret key K is comprised of a sequence of symbols of the form $K=(k_1,\ldots\ldots,k_k)$.

6. The method of Claim 1, wherein the secret key K may be determined from said (d-1) parity symbols and said response B by satisfying an inequality,

$$d_H(A,B) <= (d-1-k)/2$$

where $d_H(A,B)$ is the Hamming distance between symbol sequences A and B,
d is the minimum distance, and
k is the number of symbols in the secret key K.

7. The method of Claim 1, wherein the codeword W is a Reed-Solomon codeword.

8. The method of Claim 1, wherein the secret key K cannot be determined by someone other than said first and second correspondent (18) if the following inequality is satisfied,

$$d_H(A,E) >= d-1$$

where: E is a symbol sequence obtained by an attacker (17) attempting to learn the secret key K,
$d_H(A,E)$ is the Hamming distance between the symbol sequences A and E, and
d is the minimum distance.

9. A method of secret key agreement between a first and a second correspondent (18), the method comprising the acts of:

during an enrollment phase:

(a) sending to a source (20), a challenge C, from a first correspondent (16) at a time t1;

(b) said first correspondent (16) receiving said response A to said challenge C;

(c) sending to said source (20), said challenge, from said second correspondent (18) B at a time t2;

(d) said second correspondent (18) receiving a response B to said challenge C.

during an encoding phase, said first correspondent (16):

(a) selecting a secret key K;

(b) forming a codeword W using said secret key K and said response A to generate (d-1) parity symbols P;

(c) transmitting said (d-1) parity symbols P to said second correspondent (18) over a public communication channel;

during a decoding phase, said second correspondent (18):

(a) using said d-1 transmitted parity symbols and said response B to construct a word W' to determine the secret key K.

10. The method of Claim 9, wherein said response A is comprised of a sequence of symbols of the form $A=(a_1,\ldots\ldots a_n)$.

11. The method of Claim 9, wherein said response B is comprised of a sequence of symbols of the form $B=(b_1,\ldots\ldots,b_n)$.

12. The method of Claim 9, wherein said secret key K is comprised of a sequence of symbols of the form $K=(k_1,\ldots\ldots,k_k)$.

13. The method of Claim 9, wherein the secret key K may be determined from said word W' if and only if the inequality is satisfied

$$d_H(A,B) <= (d-1-k)/2$$

where $d_H(A,B)$ is the Hamming distance between symbol sequences A and B,
d is the minimum distance, and
k is the number of symbols in the secret key K.

14. The method of Claim 9, wherein the codeword W is a Reed-Solomon codeword.

15. The method of Claim 9, wherein the secret key K cannot be determined from someone other than said first and second correspondent (18) if and only if the following inequality is satisfied:

$$d_H(A,E) >= d-1$$

where E is a symbol sequence obtained by an attacker (17) attempting to learn the secret key K,

$d_H(A,E)$ is the Hamming distance between the symbol sequences A and E, and

d is the minimum distance.

16. A method of secret key agreement between a first and a second correspondent (18), the method comprising the acts of:

said first correspondent (16) receiving a response A from a source P (20);

said second correspondent (18) receiving a response B from said source P (20);

said first correspondent (16) generating (d-1) parity symbols as an output of a codeword W whose input includes said response A and a secret key K selected by said first correspondent (16);

said first correspondent (16) transmitting said (d-1) parity symbols and a pseudo-random function evaluated in A, over a public communication channel to said second correspondent (18); and

said second correspondent (18) generating a word W' whose input includes said (d-1) parity symbols, said pseudo-random function evaluated A, and said response B, to determine said secret key K selected by said first correspondent (16).

17. The method of Claim 16, wherein the pseudo-random function is a hash function of the form h(A)=(h(a1),...,h(an)), where A is the response A from said source P (20).

18. The method of Claim 16, wherein said response A is comprised of a sequence of symbols of the form $A=(a_1,\ldots\ldots a_n)$.

19. The method of Claim 16, wherein said response B is comprised of a sequence of symbols of the form $B=(b_1,\ldots\ldots,b_n)$.

20. The method of Claim 16, wherein said secret key K is comprised of a sequence of symbols of the form $K=(k_1,\ldots\ldots,k_k)$.

21. The method of Claim 16, wherein the secret key K may be determined from said word W' if the inequality is satisfied,

$$d_H(A,B) <= (d-1-k)$$

where $d_H(A,B)$ is the Hamming distance between symbol sequences A and B,
d is the minimum distance, and
k is the number of symbols in the secret key K.

22. The method of Claim 16, wherein the codeword W is a Reed-Solomon codeword.

23. The method of Claim 16, wherein the secret key K cannot be determined from someone other than said first and second correspondent (18)s if the following inequality is satisfied:

$$d_H(A,E) >= d-1$$

where E is an attacker (17) attempting to learn the secret key K,
$d_H(A,E)$ is the Hamming distance between the symbol sequences A and E, and
d is the minimum distance.

24. A method of secret key agreement between a first and a second correspondent (18), the method comprising the acts of:

during an enrollment phase:

sending to a source (20), a challenge C, from said first correspondent (16) at a time t1;

receiving said response A to said challenge C;

sending to said source (20), said challenge C, from said second correspondent (18) at a time t2;

during an encoding phase:

said first correspondent (16) selecting a secret key K;

forming a codeword W using said secret key K, a response A received by said first correspondent (16) during an enrollment phase and d-1 parity symbols P;

transmitting said d-1 parity symbols P and h(A) a pseudo-random function of A from said first correspondent (16) to said second correspondent (18) over a public communication channel;

during a decoding phase:

using said d-1 transmitted parity symbols and said pseudo-random function evaluated in A by said second correspondent (18) to construct a word W' to determine the secret key K.

25. The method of Claim 24, wherein the pseudo-random function is a hash function h(A)=(h(a_1),...,h(a_n))

26. The method of Claim 24, wherein said response A is comprised of a sequence of symbols of the form $A=(a_1,.....a_n)$.

27. The method of Claim 24, wherein said response B is comprised of a sequence of symbols of the form $B=(b_1,.....,b_n)$.

28. The method of Claim 24, wherein said secret key K is comprised of a sequence of symbols of the form $K=(k_1,\ldots\ldots,k_k)$.

29. The method of Claim 24, wherein the secret key K may be determined from said word W' if the inequality is satisfied,

$$d_H(A,B) <= (d-1-k)$$

where $d_H(A,B)$ is the Hamming distance between symbol sequences A and B,
d is the minimum distance, and
k is the number of symbols in the secret key K.

30. The method of Claim 24, wherein the codeword W is a Reed-Solomon codeword.

31. The method of Claim 24, wherein the secret key K cannot be determined from someone other than said first and second correspondents (16,18) if the following inequality is satisfied:

$$d_H(A,E) >= d-1$$

where E is a symbol sequence obtained by an attacker (17) attempting to learn the secret key K,
$d_H(A,E)$ is the Hamming distance between the symbol sequences A and E, and
d is the minimum distance.

32. A method of secret key agreement between a first and a second correspondent (18), the method comprising the acts of:
said first correspondent (16) receiving a response A from a source P (20), where A is a set of symbols;
said second correspondent (18) receiving a response B from said source P (20), where B is a set of symbols;

said first correspondent (16) ordering the set of symbols A into a sequence, $a_1,\ldots\ldots,a_N$;

said first correspondent (16) computing a pseudo-random function of the ordered set of symbols A, h(A);

said first correspondent (16) transmitting h(A)=(h(a1),...h(an)) to said second correspondent (18); and;

said second correspondent (18) computing a pseudo-random function of the ordered set of symbols B, h(b) for each symbol b in the set B;

said second correspondent (18) computing a set S which includes all positions j for which there exists an element in B such that $h(a_j) = h(b)$;

said second correspondent (18) transmitting the set S back to said first correspondent (16); and

both first and second correspondents (16, 18) extracting a joint key J based on the symbols a_j, j in S and for those symbols b in set B for which $h(a_j) = h(b)$.

33. The method of Claim 32, further comprising the act of extracting a secret key K from said joint key J using privacy amplification.

34. The method of Claim 33, wherein using said privacy amplification includes using one of a random matrix multiplier for multiplication with the joint key J and the joint key J evaluated in a hash function.

35. The method of Claim 32, wherein said responses A and B are received by said respective first (16) and second (18) correspondents responsive to a challenge C generated from said respective first (16) and second (18) correspondents.

36. The method of Claim 32, wherein said response A is comprised of a sequence of symbols of the form $A=(a_1,\ldots\ldots a_n)$.

37. The method of Claim 32, wherein said response B is comprised of a sequence of symbols of the form $B=(b_1,\ldots\ldots,b_n)$.

38. The method of Claim 32, wherein said secret key K is comprised of a sequence of symbols of the form $K=(k_1,\ldots\ldots,k_k)$.